IN THE DRAWINGS:

Applicants have submitted formal drawings labeled Figures 1-6 to replace the hand drawn drawings on file, as suggested by the Office Action.

IN THE SPECIFICATION:

Please replace the paragraph in the specification beginning on page 1, line 7, with the following paragraph:

> PDA PASSWORD MANAGEMENT TOOL, 10/042,095~~(Internal Docket Number AUS920010598US1)~~, filed even date herewith, and commonly assigned, is hereby incorporated by reference.

Please replace the paragraph in the specification beginning on page 3, line 20, with the following paragraph:

> Other users may utilize a password management tool that automatically accesses a database that contains the passwords for each secure resource. Depending on the number of resources and passwords, this may require more memory than what is available if a mobile device is used for storing passwords as described in co-pending US Patent Application Serial Number 10/042,095 ~~(Internal Docket Number AUS920010598US1)~~. If a mobile device is not used for storing the user's passwords, then the user's use of the database may be limited to the times in which the user is accessing the resources from the computer on which the database resides. Otherwise, the user would need to access the database over a network. Nevertheless, the user still has the burden of updating the database when passwords expire, or adding passwords when new resources are accessed. Furthermore, the password security may be compromised if the database is ever broken into.

Please replace the paragraph in the specification beginning on page 11, line 16, with the following paragraph:

With reference to Fig. 2, the system, method and program of the present invention generates and maintains encrypted passwords. A preferred embodiment of the invention is an application programming tool 201 running on a client 220 which generates different passwords 230, 240, 250, 260 for a user that are needed for the different Internet sites visited by the user which require a password; or for any resource, such as another application program such as Lotus Notes, which requires a password. Windows 213, 214, 215, 216 display the Internet sites from servers 203, 204, 205, 206, respectively. Although Fig. 2 illustrates that the Internet sites or resources are located on separate servers 203, 204, 205, 206, one or more of the resources could be located on the same server. It should be noted that in a preferred embodiment of the invention, the resources have a user interface, such as user interface 226, for querying the user for a user ID [[~~id~~]] and a password.

Please replace the paragraph in the specification beginning on page 13, line 20, with the following paragraph:

The set of global hash keys 420 (Fig. 4) ~~generate~~ generates the set of passwords 231-236 shown in Fig. 3. For example, the first time that a first password 231 is generated for a site, it is the first iteration. When the first password 231 expires, a second password 232 is generated which is referred to herein as the second iteration. The third iteration occurs when the second password 232 expires and a third password 233 is generated, and so on. If there are only six global keys in the set, then after the sixth password 236 expires, the cycle returns to the first iteration and the first password 231 is regenerated using the first global key. This allows a password from a set of passwords to be used again at a later time for the same single resource, such as a resource at server A 203.

Please replace the paragraph in the specification beginning on page 18, line 3, with the following paragraph:

Fig. 5A illustrates a process flow and logic of a preferred embodiment of the invention. The process begins at step 501, when a user invokes the tool of the present invention during a given computing session on a computer on which the tool is executing. The tool receives as user input the user's user ID [[~~id~~]], the user's global password, and the set of global keys or hash values, 502. In a preferred embodiment, the tool receives the user input each time the user uses the client for a different computing session to minimize any non volatile storage requirements of the tool. In other embodiments, the set of hash values are stored for a particular user by user id and global user password. When a user accesses the tool, the user would then only have to input the user's user ID [[~~id~~]] and global password. The tool would then have access to the set of hash values stored for that user.

Please replace the paragraph in the specification beginning on page 18, line 19, with the following paragraph:

Then, when a user accesses a resource, such as a domain, that is requesting a user ID [[~~id~~]] and password, the user invokes the password generation function of the tool. For example, the user may select a button within a user interface of the tool running in a separate frame or window on the user's system. If the password generation function is invoked 503, the tool determines the resource domain name 504 being accessed; and uses the domain name, the global user password, and the hash value to generate a password 505. The tool then populates the resource with the generated password 506.

Please replace the paragraph in the specification beginning on page 19, line 1, with the following paragraph:

Fig. 5B illustrates a process flow and logic of yet another embodiment of the invention. After receiving the user's initial input 502, the tool automatically recognizes when a password is being requested 513. The tool determines the domain or resource name 514. When the domain is determined, the tool may access a database 600 (Fig. 6) that the tool has built in order to determine the iteration 612 of password generation that the tool has undertaken for the determined domain name 611. Referring back to Fig 5B, ~~Fig. 5,~~ once the iteration for that domain is determined 515, the corresponding hash value in the sequence of hash values for that iteration are determined 516. The tool generates the password from the domain name, the determined hash value, and the global user password 517. The tool determines whether the resource has a required format for the password 518 such as by examining format field 613 in database 600 for that resource 611 (Fig. 6). If it does, then the tool forces the generated password to conform to the format. The process continues such that the tool then automatically populates the domain with the generated password for that domain and for that iteration of the password 520.

Please replace the paragraph in the specification beginning on page 20, line 4, with the following paragraph:

In one implementation of this invention, the tool can be installed on a remote device as described in co-pending U.S. Application Serial Number 10/042,095 ~~(Internal Docket Number AUS920010598US1)~~. For further security, it may be desirable for the user to utilize the user's user ID [[~~id~~]] and/or global password as a sign on to get access to the remote device or to get access to the tool thereon. The tool may also have stored therein a user profile having the set of global values, i.e., hash values. As such, instead of using a remote device to store a large number of passwords for all of the resources utilized by the user, the remote device would merely contain the tool that could generate the needed password on demand.